HP TCP/IP Services for OpenVMS

Release Notes

September 2003

This document describes the new features and changes to the HP TCP/IP Services for OpenVMS Version 5.4 software product.

Revision/Update Information:	This is a new document.
Software Version:	HP TCP/IP Services for OpenVMS Version 5.4
Operating Systems:	HP OpenVMS Alpha Versions 7.3-1 and 7.3-2

Hewlett-Packard Company
Palo Alto, California

The HP TCP/IP Services for OpenVMS documentation is available on CD-ROM.

This document was prepared using DECdocument, Version 3.3-1b.

Contents

3 Problems and Restrictions

4 Corrections

5 Documentation Update

Tables

Preface

The HP TCP/IP Services for OpenVMS product is the HP implementation of the TCP/IP protocol suite and internet services for OpenVMS Alpha and OpenVMS VAX systems. This document describes the HP TCP/IP Services for OpenVMS Version 5.4 product.

TCP/IP Services provides a comprehensive suite of functions and applications that support industry-standard protocols for heterogeneous network communications and resource sharing.

For installation instructions, see the *HP TCP/IP Services for OpenVMS Installation and Configuration* manual.

The release notes provide version-specific information that supersedes the information in the documentation set. The features, restrictions, and corrections in this version of the software are described in the release notes. Always read the release notes before installing the software.

Intended Audience

These release notes are intended for experienced OpenVMS and UNIX® system managers and assumes a working knowledge of OpenVMS system management, TCP/IP networking, TCP/IP terminology, and some familiarity with the TCP/IP Services product.

Related Documents

Table 1 lists the documents available with this version of TCP/IP Services.

Table 1 TCP/IP Services Documentation

Manual	Contents
Compaq TCP/IP Services for OpenVMS Concepts and Planning	This manual provides conceptual information about TCP/IP networking on OpenVMS systems, including general planning issues to consider before configuring your system to use the TCP/IP Services software. This manual also describes the other manuals in the TCP/IP Services documentation set and provides a glossary of terms and acronyms for the TCP/IP Services software product.
HP TCP/IP Services for OpenVMS Release Notes	The release notes provide version-specific information that supersedes the information in the documentation set. The features, restrictions, and corrections in this version of the software are described in the release notes. Always read the release notes before installing the software.

(continued on next page)

Table 1 (Cont.) TCP/IP Services Documentation

Manual	Contents
HP TCP/IP Services for OpenVMS Installation and Configuration	This manual explains how to install and configure the TCP/IP Services product.
HP TCP/IP Services for OpenVMS User's Guide	This manual describes how to use the applications available with TCP/IP Services such as remote file operations, e-mail, TELNET, TN3270, and network printing.
HP TCP/IP Services for OpenVMS Management	This manual describes how to configure and manage the TCP/IP Services product.
HP TCP/IP Services for OpenVMS Management Command Reference	This manual describes the TCP/IP Services management commands.
HP TCP/IP Services for OpenVMS Management Command Quick Reference Card	This reference card lists the TCP/IP management commands by component and describes the purpose of each command.
HP TCP/IP Services for OpenVMS UNIX Command Equivalents Reference Card	This reference card contains information about commonly performed network management tasks and their corresponding TCP/IP management and Tru64 UNIX command formats.
Compaq TCP/IP Services for OpenVMS ONC RPC Programming	This manual presents an overview of high-level programming using open network computing remote procedure calls (ONC RPC). This manual also describes the RPC programming interface and how to use the RPCGEN protocol compiler to create applications.
HP TCP/IP Services for OpenVMS Guide to SSH	This manual describes how to configure, set up, use, and manage the SSH for OpenVMS software.
Compaq TCP/IP Services for OpenVMS Sockets API and System Services Programming	This manual describes how to use the Sockets API and OpenVMS system services to develop network applications.
Compaq TCP/IP Services for OpenVMS SNMP Programming and Reference	This manual describes the Simple Network Management Protocol (SNMP) and the SNMP application programming interface (eSNMP). It describes the subagents provided with TCP/IP Services, utilities provided for managing subagents, and how to build your own subagents.
HP TCP/IP Services for OpenVMS Tuning and Troubleshooting	This manual provides information about how to isolate the causes of network problems and how to tune the TCP/IP Services software for the best performance. It also provides information about using UNIX network management utilities on OpenVMS.
HP TCP/IP Services for OpenVMS Guide to IPv6	This manual describes the IPv6 environment, the roles of systems in this environment, the types and function of the different IPv6 addresses, and how to configure TCP/IP Services to access the IPv6 network.

For additional information about HP OpenVMS products and services, visit the following World Wide Web address:

`http://www.hp.com/go/openvms`

For a comprehensive overview of the TCP/IP protocol suite, refer to the book *Internetworking with TCP/IP: Principles, Protocols, and Architecture*, by Douglas Comer.

Reader's Comments

HP welcomes your comments on this manual. Please send comments to either of the following addresses:

Internet	**openvmsdoc@hp.com**
Postal Mail	Hewlett-Packard Company OSSG Documentation Group, ZKO3-4/U08 110 Spit Brook Rd. Nashua, NH 03062-2698

How to Order Additional Documentation

For information about how to order additional documentation, visit the following World Wide Web address:

`http://www.hp.com/go/openvms/doc/order`

Conventions

In the product documentation, the name TCP/IP Services means both:

- HP TCP/IP Services for OpenVMS Alpha
- HP TCP/IP Services for OpenVMS VAX

In addition, please note that all IP addresses are fictitious.

The following conventions are used in the documentation.

Ctrl/*x*	A sequence such as Ctrl/*x* indicates that you must hold down the key labeled Ctrl while you press another key or a pointing device button.
PF1 *x*	A sequence such as PF1 *x* indicates that you must first press and release the key labeled PF1 and then press and release another key or a pointing device button.
Return	In examples, a key name enclosed in a box indicates that you press a key on the keyboard. (In text, a key name is not enclosed in a box.) In the HTML version of this document, this convention appears as brackets, rather than a box.
. . .	A horizontal ellipsis in examples indicates one of the following possibilities: • Additional optional arguments in a statement have been omitted. • The preceding item or items can be repeated one or more times. • Additional parameters, values, or other information can be entered.
. . .	A vertical ellipsis indicates the omission of items from a code example or command format; the items are omitted because they are not important to the topic being discussed.

( )	In command format descriptions, parentheses indicate that you must enclose choices in parentheses if you specify more than one.
[ ]	In command format descriptions, brackets indicate optional choices. You can choose one or more items or no items. Do not type the brackets on the command line. However, you must include the brackets in the syntax for OpenVMS directory specifications and for a substring specification in an assignment statement.
|	In command format descriptions, vertical bars separate choices within brackets or braces. Within brackets, the choices are optional; within braces, at least one choice is required. Do not type the vertical bars on the command line.
{ }	In command format descriptions, braces indicate required choices; you must choose at least one of the items listed. Do not type the braces on the command line.
bold type	Bold type represents the introduction of a new term. It also represents the name of an argument, an attribute, or a reason.
italic type	Italic type indicates important information, complete titles of manuals, or variables. Variables include information that varies in system output (Internal error *number*), in command lines (/PRODUCER=*name*), and in command parameters in text (where *dd* represents the predefined code for the device type).
UPPERCASE TYPE	Uppercase type indicates a command, the name of a routine, the name of a file, or the abbreviation for a system privilege.
`Example`	This typeface indicates code examples, command examples, and interactive screen displays. In text, this type also identifies URLs, UNIX commands and pathnames, PC-based commands and folders, and certain elements of the C programming language.
-	A hyphen at the end of a command format description, command line, or code line indicates that the command or statement continues on the following line.
numbers	All numbers in text are assumed to be decimal unless otherwise noted. Nondecimal radixes—binary, octal, or hexadecimal—are explicitly indicated.

1
New Features and Changes

This chapter describes the new features of HP TCP/IP Services for OpenVMS Version 5.4.

Note

TCP/IP Services V5.4 is supported on OpenVMS Alpha systems only.

For more information about configuring and managing these services, see the *HP TCP/IP Services for OpenVMS Management* guide provided with the TCP/IP Services software.

Table 1–1 lists the new features of TCP/IP Services Version 5.4 and the sections that describe them.

Table 1–1 TCP/IP for OpenVMS Version 5.4 New Features

Section	Description
Section 1.1	A new TCP/IP kernel provides performance scalability for symmetric multiprocessing (SMP) systems.
Section 1.2	Secure shell (SSH) client and server.
Section 1.3	Secure Socket Layer (SSL) for POP.
Section 1.4	IP address failover.
Section 1.5	Software update and new programming examples using IPv6 APIs.
Section 1.6	BIND server Version 9.2.1.
Section 1.7	INET driver performance enhancements.
Section 1.8	NFS server performance enhancements.
Section 1.9	TELNET server performance enhancements.
Section 1.10	BG device creation enhancement.
Section 1.11	Fast BG device creation and deletion.
Section 1.12	Updated standard kernel.
Section 1.13	Support for TCPDUMP utility.

1.1 Scalable Kernel

The TCP/IP kernel has been modified to provide increased performance on symmetric multiprocessing (SMP) systems.

This complete redesign of the TCP/IP kernel provides enhanced performance on SMP systems by removing CPU contention among users. The new kernel uses a dynamic spinlock to lock the main internal database. All processing that requires locking is directed to a designated TCP/IP CPU, thus eliminating CPU contention with other CPU users. Essentially, network I/O becomes a series of asynchronous, transaction-based operations.

Note

Be aware that implementations of the scalable kernel in future versions of TCP/IP Services may differ from the way it is described here. Always consult the current documentation.

1.1.1 Enabling the Scalable Kernel

To enable the scalable kernel, add the following lines to the SYS$MANAGER:SYLOGICALS.COM command procedure:

```
$ ! ONLY the argument "PERF=ALL" is supported.
$ ! Other values may cause unpredictable results
$ ! to disable scalable kernel support, comment out next line and reboot.
$ DEFINE/SYSTEM/EXECUTIVE TCPIP$STARTUP_CPU_IMAGES "PERF=ALL"
```

If TCP/IP Services has already been started, you must reboot the system after you make this change to the SYLOGICALS.COM file.

Although the scalable kernel runs on single processor systems, its greatest benefits are derived from its use on symmetric multiprocessor (SMP) systems.

When the scalable kernel is enabled, the following messages are displayed when TCPIP$STARTUP.COM is executed:

```
%TCPIP-I-INFO, PERF cpu-specific image SYS$LOADABLE_IMAGES:TCPIP$BGDRIVER_PERF.EXE selected
%TCPIP-I-INFO, PERF cpu-specific image SYS$LOADABLE_IMAGES:TCPIP$INTERNET_SERVICES_PERF.EXE selected
%TCPIP-I-INFO, PERF cpu-specific image SYS$SYSTEM:TCPIP$INETACP_PERF.EXE selected
%TCPIP-I-INFO, PERF cpu-specific image SYS$LOADABLE_IMAGES:TCPIP$TNDRIVER_PERF.EXE selected
```

To verify that the scalable kernel is enabled, use the TCP/IP management command SHOW VERSION/ALL. The value of the TCPIP$STARTUP_CPU_ IMAGES logical name is displayed. Images pertinent to the scalable kernel will have a _PERF suffix. Also, the image identification will have a PF suffix.

1.1.2 Restrictions on Using the Scalable Kernel

When you enable the scalable kernel, be aware of the following:

- The Point-to-Point Protocol (PPP) and Serial Line Protocol (SLIP) do not work when the scalable kernel is running.
- When you select the scalable kernel, the following `net` subsystem attributes are modified:
  - The `ovms_unit_maximum` attribute is set to 32767.
  - The `ovms_unit_fast_credel` attribute is set to 1, or ON.
  - The `ovms_unit_minimum` attribute is set to 2.

  These changes enable your system to exceed 9999 BG device sockets, since many more are required for high-performance systems with multiple CPUs. For more information about these attributes, refer to the *HP TCP/IP Services for OpenVMS Tuning and Troubleshooting* manual.

- When you use the scalable kernel, certain operations with the `tcpdump` utility may fail. For example, it is not possible to trace ARP packets.

1.2 Secure Shell (SSH)

This release includes the Secure Shell (SSH) client and server, providing secure login, remote command execution, and file transfer. This implementation is based on SSH2 software from SSH Communications Security Corp., Version 2.4.1.

Note

If the TCP/IP Services V5.3 Early Adopter's Kit (EAK) for SSH for OpenVMS is installed on the system, you must use the PCSI command PRODUCT REMOVE to remove the EAK before you install TCP/IP Services V5.4.

The SSH server allows:

- Remote users to securely log in to the system.
- Secure file transfers between remote computers.
- Remote command execution.

For information about configuring, managing, and using SSH for OpenVMS, refer to the *HP TCP/IP Services for OpenVMS Guide to SSH*.

For restrictions on the use of this version of SSH for OpenVMS, see Section 3.5.

1.3 Secure POP

SSL (Secure Socket Layer) is supported for POP (Post Office protocol), providing secure retrieval of mail.

The secure POP server accepts connections on port 995. Secure POP encrypts passwords, data, and POP commands and is compatible with clients that use SSL, such as Microsoft Outlook.

To use this feature, you must download the HP SSL kit for OpenVMS Alpha from:

`http://www.openvms.compaq.com/openvms`

Select "Security Products."

If the HP SSL software is not installed, the POP server will communicate in non-SSL mode.

For information about configuring and managing Secure POP, see the *HP TCP/IP Services for OpenVMS Management* guide.

The SSL logical names are defined by the SSL startup procedure. Therefore, if you have POP configured to use SSL logical names to locate the certificate and key files, you must ensure that the SSL startup procedure is run before the TCP/IP Services startup procedure.

1.4 failsafe IP

The failSAFE IP feature provides IP address failover capability for multiple interfaces on a host or a cluster.

Note

If you have installed the TCP/IP Services V5.3 Early Adopter's Kit (EAK) for failSAFE IP, you must use the PCSI command PRODUCT REMOVE to remove the EAK before you install TCP/IP Services V5.4.

For more information about configuring and managing failSAFE IP, see the *HP TCP/IP Services for OpenVMS Management* guide.

For information about restrictions on using this version of failSAFE IP, see Section 3.2.

1.5 IPv6 Enhancements

The following sections describe updates and enhancements to IPv6 functionality.

1.5.1 IPv6 DNS Domain Name and Address Registration

New with this release, the TCPIP$ND6HOST process is capable of registering the host's domain name and address in the DNS.

The TCPIP$ND6HOST process receives and processes IPv6 Router Advertisement (RA) packets of the Neighbor Discovery Protocol. This enables a system to autoconfigure itself without manual intervention. With this version of TCP/IP Services, you can also enable DNS registration.

To enable host name and address registration, enter the following command:

```
$ DEFINE /SYSTEM TCPIP$ND6D_ENABLE_DDNS 1
```

The domain name to be registered is obtained using the `gethostname()` call.

To update the zone, TCPIP$ND6HOST sends dynamic updates to the primary master name server. The name of the primary master name server is stored in the MNAME field of the SOA record for a zone. To determine the master name server, TCPIP$ND6HOST sends a query for the zone's SOA record to the name server specified in the DNS resolver configuration. To display the DNS resolver configuration information, use the TCP/IP management command SHOW NAME.

To make use of this feature, you must enable dynamic updates. By default, dynamic updates are rejected by DNS servers. For information about allowing dynamic updates, see the BIND Chapter of the *HP TCP/IP Services for OpenVMS Management* guide.

1.5.2 IPv6 API Updates

The IPv6 programming APIs have been updated. New programming examples are provided with this release. The following is a list of the specific changes to the IPv6 APIs:

- IPv6 Changes:
  - The flag value AI_DEFAULT, which could previously be specified in the `ai_flags` parameter for a call to the `getaddrinfo` function, has been deprecated. It will be removed from the NETDB.H file in a future release.

To achieve the behavior defined by this flag, specify the logical OR of the flag values AI_V4MAPPED and AI_ADDRCONFIG.

- The BIND resolver has been updated as described in the following RFC draft:

  `draft-ietf-ipngwg-scoping-arch-04.txt`

  This change allows the specification of an IPv6 nonglobal address without ambiguity by also specifying an intended scope zone. The format is as follows:

  address%zone_id

  The format of the nonglobal address includes the following:

  - *address* is a literal IPv6 address
  - *zone_id* is a string to identify the zone of the address
  - % is a delimiter character to distinguish between the address and zone identifier.

  For example, the following specifies a nonglobal address on interface WE0:

  `fe80::1234%WE0`

- The IPv4 TCP and UDP client and server C socket programming example programs that reside in SYS$COMMON:[SYSHLP.EXAMPLES.TCPIP] have been ported to IPv6. The IPv6 versions of these example programs are located in SYS$COMMON:[SYSHLP.EXAMPLES.TCPIP.IPV6].
- The IPv6 example database and configuration files in SYS$COMMON:[SYSHLP.EXAMPLES.TCPIP.IPV6.BIND] have been updated to reflect current practice.

For more information about using the IPv6 APIs, refer to the *HP TCP/IP Services for OpenVMS Guide to IPv6*.

1.6 BIND Version 9.2.1

The BIND server has been updated from Version 9.2.0 to Version 9.2.1. This update provides corrections to problems in the previous version of the software.

1.7 Performance Enhancements to the INET Driver

For Alpha systems only, the INETDRIVER now uses the faster internal interface to the TCP/IP networking kernel. The impact on nonpaged pool consumption and process quotas is now greatly reduced.

1.8 Performance Enhancements to the NFS Server

The NFS server now caches the contents of directory files, in addition to the content of other files. The server must access the directory files to cache them.

For information about managing the NFS directory cache, see the *HP TCP/IP Services for OpenVMS Management* guide.

1.9 Performance Enhancements to the TELNET Server

The TELNET/RLOGIN server (TNDRIVER) has been improved as follows:

- The amount of CPU overhead required for maintaining the TN devices has been reduced.
- IOLOCK8 spinlocks are no longer used.
- Concurrent operation of TN devices has been added.

1.10 Support for More Than 10,000 BG Devices

This feature allows a system, such as a web server, to have more than 10,000 devices. To enable this feature, set the following `net` subsystem attribute to a value from 9999 to 32767:

```
ovms_unit_maximum
```

This subsystem attribute must be defined in the SYSCONFIGTAB.DAT. For more information about modifying the SYSCONFIGTAB.DAT file, see the *HP TCP/IP Services for OpenVMS Tuning and Troubleshooting* guide.

1.11 Support for Fast BG Device Creation and Deletion

To support systems where large numbers of BG devices are continuously being created and deleted, as well as systems where the number of BG devices has been increased above the default 10,000 device unit limit, a new subsystem attribute enables fast creation and deletion of BG devices:

```
ovms_unit_fast_credel
```

The default setting for this attribute is 0, or OFF. This attribute must be defined in the SYSCONFIGTAB.DAT file. For more information about modifying the SYSCONFIGTAB.DAT file, see the *HP TCP/IP Services for OpenVMS Tuning and Troubleshooting* guide.

1.12 Updated TCP/IP Kernel

The TCP/IP Services kernel has been updated to Tru64 UNIX 5.1B.

1.13 tcpdump Support

This version of TCP/IP Services includes the `tcpdump` utility. The `tcpdump` utility provides dump analysis and packet capturing. Specifically:

- Native packet tracing and file-based tracing
- Native tracing in copy-all mode (no promiscuous support)
- Filter expression (boolean-based). For example:

```
$ tcpdump ip host lassie and (port 21 or port 20)
```

For information about using the `tcpdump` utility, see the *HP TCP/IP Services for OpenVMS Tuning and Troubleshooting* guide.

2

Installation, Configuration, and Startup Notes

Use this chapter in conjunction with the *HP TCP/IP Services for OpenVMS Installation and Configuration* manual.

2.1 Installing Over V5.3 Early Adopter's Kits (EAKs)

If you have installed one or more of the following V5.3 EAKs, you must use the PCSI REMOVE command to remove the EAKs before you install TCP/IP Services V5.4:

- SSH for OpenVMS EAK
- failSAFE IP EAK

Note

If you install the current TCP/IP Services version after removing the failSAFE IP EAK, you must run TCPIP$CONFIG.COM to reestablish your target and home interfaces.

2.2 Installation Changes

The TCPIP$VMS_FILES.DOC file is no longer included in the installation of the TCP/IP Services software kit.

2.3 Configuring IPv6

The following sections describe procedures specific to systems where IPv6 is to be enabled.

2.3.1 Information for Users of the IPv6 Early Adopter's Kit

If you are running any version of the TCP/IP Services V5.0 IPv6 EAK, remove the EAK and then install the current version of the TCP/IP Services software. You must then run the TCPIP$IP6_SETUP.COM command procedure. For more information, refer to the *HP TCP/IP Services for OpenVMS Guide to IPv6*.

The definition of a `sockaddr` structure has been changed. This change breaks binary compatibility for IPv6 applications that were compiled using the TCP/IP Services Version 5.0 EAK. You must recompile and relink your applications after you install the current version of TCP/IP Services.

2.3.2 Warning Message in TCPIP$CONFIG.COM

If you have run the TCPIP$IP6_SETUP.COM procedure to enable IPv6, and then you run the TCPIP$CONFIG.COM command procedure, TCPIP$CONFIG.COM displays the following warning message when you select the `Core environment` option:

```
                        WARNING

This node has been configured for IPv6.  If you make any additional
changes to the configuration of the interfaces, you must run
TCPIP$IP6_SETUP again and update your host name information in
BIND/DNS for the changes to take effect.
```

2.4 Startup Problems and Restrictions

The following list describes the restrictions on starting TCP/IP Services:

- Booting OpenVMS with MIN, INST, or UPGRADE is not supported. The product configuration and startup command procedures (TCPIP$CONFIG.COM and TCPIP$STARTUP.COM) fail if you perform any kind of boot other than a full boot.
- The TCPIP$CONFIG.COM command procedure fails on systems that do not have a SYSUAF database and a RIGHTSLIST database. These OpenVMS files must be created before you configure TCP/IP Services.

2.5 Upgrading from TCP/IP Services Version 4.*x*

The following sections describe how to preserve the behavior of the software when you upgrade from an older version of TCP/IP Services (UCX) to the current version.

2.5.1 Upgrading LPD

- When you merge edits into the system startup command procedure, do not include the commands to start and stop the queue UCX$LPD_QUEUE. This queue has been replaced with TCPIP$LPD_QUEUE. The commands for starting and stopping TCPIP$LPD_QUEUE are in the LPD startup and shutdown command procedure files.
- After you merge the edits, modify the value of the /PROCESSOR qualifier in the LPD client queue startup commands that you have just appended, replacing UCX$LPD_SMB with TCPIP$LPD_SMB. For example, enter the following command:

  ```
  LSE Command> SUBSTITUTE/ALL "ucx$lpd_smb" "tcpip$lpd_smb"
  ```

2.5.2 Saving Mail Messages When You Upgrade

The new version of SMTP includes control files that are different from previous versions. Before upgrading to the current version of TCP/IP Services, use the TCP/IP management command ANALYZE MAIL to pick up any dead letters (SMTP control files that have not been submitted to a print queue). For example:

```
$ TCPIP ANALYZE MAIL/REPAIR
```

2.5.3 Preserving SNMP Startup and Shutdown Behavior

After you upgrade to the current version of TCP/IP Services, you must perform one of the following actions to ensure correct SNMP startup:

- If SNMP was configured under an old TCP/IP Services installation (UCX) and you want to retain the previous configuration, run the SYS$MANAGER:TCPIP$CONFIG.COM command procedure and select the option to automatically convert UCX configuration files.
- After you upgrade to the current version of TCP/IP Services, run the SYS$MANAGER:TCPIP$CONFIG.COM command procedure. If SNMP is still enabled, disable SNMP then enable it again. This is necessary for the proper operation of this component.

If you have customized versions of the UCX$SNMP_STARTUP.COM and UCX$SNMP_SHUTDOWN.COM command procedures (used to start and stop extension subagents), save your customized files to a different directory before upgrading to the new version of TCP/IP Services. If you do not perform this step, your customized changes will be lost.

Check for versions of these files in the following locations:

- SYS$MANAGER
- SYS$STARTUP
- SYS$SYSDEVICE:[UCX$SNMP]

After you install TCP/IP Services, manually enter commands into the TCPIP$SNMP_SYSTARTUP.COM and TCPIP$SNMP_SYSHUTDOWN.COM command procedures, as described in the *HP TCP/IP Services for OpenVMS Management* guide.

2.5.4 Customizing SNMP Startup and Shutdown

Enabling SNMP using the TCPIP$CONFIG.COM command procedure no longer creates the following files:

- TCPIP$SNMP_SYSTARTUP.COM
- TCPIP$SNMP_SYSHUTDOWN.COM

These command procedures are used for starting and stopping custom SNMP subagents. They will not be affected by installing future versions of TCP/IP Services.

2.5.5 SNMP Messages When You Install TCP/IP Services

For sites where the same version of TCP/IP Services is installed multiple times, informational messages similar to the following may appear in the installation dialog:

```
Do you want to review the options? [NO]

Execution phase starting ...
```

```
The following product will be installed to destination:
    DEC AXPVMS TCPIP T5.3-9I              DISK$AXPVMSSYS:[VMS$COMMON.]
The following product will be removed from destination:
    DEC AXPVMS TCPIP T5.3-9H              DISK$AXPVMSSYS:[VMS$COMMON.]
%PCSI-I-RETAIN, file [SYSEXE]TCPIP$ESNMP_SERVER.EXE was not replaced because
file from kit does not have higher generation number
%PCSI-I-RETAIN, file [SYSEXE]TCPIP$HR_MIB.EXE was not replaced because file
from kit does not have higher generation number
%PCSI-I-RETAIN, file [SYSEXE]TCPIP$OS_MIBS.EXE was not replaced because file
from kit does not have higher generation number
%PCSI-I-RETAIN, file [SYSLIB]TCPIP$ESNMP_SHR.EXE was not replaced because file
from kit does not have higher generation number
%PCSI-I-RETAIN, file [SYSLIB]UCX$ESNMP_SHR.EXE was not replaced because file
from kit does not have higher generation number
```

You can ignore these messages.

2.5.6 SNMP Subagent Startup Messages

The SNMP startup procedure can produce the following error messages in subagent log files:

```
25-JUL-2001 14:13:32.47 **ERROR ESNMP_INIT.C line 3777: Could not
connect to master: connection refused
25-JUL-2001 14:13:32.94 WARNING OS_MIBS.C line 942: Master agent
cannot be reached.  Waiting to attempt reconnect.
```

These messages are the result of a timing problem and can be ignored.

2.6 Troubleshooting SMTP and LPD Shutdown Problems

If SMTP or LPD shutdown generates errors indicating that the queue manager is not running, check your site-specific shutdown command procedure (VMS_SYSHUTDOWN.COM). If this procedure contains the command to stop the queue manager (STOP/QUEUE/MANAGER), make sure this command is after the command that runs the TCPIP$SHUTDOWN.COM command procedure.

Note

You do not have to stop the queue manager explicitly. The queue manager is automatically stopped and started when you restart the system.

3
Problems and Restrictions

This chapter provides information about problems and restrictions in the current version of TCP/IP Services

3.1 Advanced Programming Environment Restrictions and Guidelines

If you use the TCP/IP advanced programming features, you should keep the following in mind:

- The header files provided in TCPIP$EXAMPLES are provided as part of our advanced TCP/IP programming environment. The following list describes restrictions and guidelines for using them:
  - Use of the functions and data structures described in TCPIP$EXAMPLES:RESOLV.H is limited to 32-bit pointers. The underlying implementation will only handle 32-bit pointers. Previously, 64-bit pointers were wrongly accepted, resulting in undefined behavior for the underlying implementation.
  - IP.H and IP6.H are header files that are incomplete in the OpenVMS environment. They contain `include` directives for header files that are not provided in this version of TCP/IP Services.
  - NAMESER.H and RESOLV.H contain transliterations that intercept calls made to nameserver and resolver API routines and redirect them to TCPIP$LIB.OLB. If you wish to use an implementation of these routines other than the one provided by TCP/IP Services, define the following symbols:

    __TCPIP_NO_NS_TRANSLITERATIONS for the nameserver API routines.

    __TCPIP_NO_RES_TRANSLITERATIONS for the resolver API routines.
- Problems with the basic socket API

  The routines `getaddrinfo`, `getnameinfo`, and `freeaddrinfo`, which are described as part of the Basic Socket Interface Extensions for IPv6 (RFC 2553bis), are not thread-safe.

3.2 failSAFE IP Restrictions

After an interface failure has occurred, the TCP/IP management command SHOW INTERFACE will not display pseudo interface addresses. Users of failSAFE IP must use the `ifconfig` utility to view IP addresses. For more information about using failSAFE IP, refer to the *HP TCP/IP Services for OpenVMS Management* guide.

3.3 BIND/DNS Restrictions

BIND Version 9 has the following restrictions when using DNSSEC:

- Certain BIND server implementations do not support AAAA (IPv6 address) records. When queried for a AAAA (IPv6) record type by the BIND resolver, these name servers will return an NXDOMAIN status, even if an A (IPv4) record exists for the same domain name. These name servers should be returning NOERROR as the status for such a query. This problems can result in delays during host name resolution.

  BIND Version 9.2.1, which is supported with this version of TCP/IP Services does not exhibit this problem.

- Serving secure zones

  When acting as an authoritative name server, BIND Version 9 includes KEY, SIG, and NXT records in responses as specified in RFC 2535 when the request has the DO flag set in the query.

  Response generation for wildcard records in secure zones is not fully supported. Responses indicating the nonexistence of a name include a NXT record proving the nonexistence of the name itself, but do not include any NXT records to prove the nonexistence of a matching wildcard record. Positive responses resulting from wildcard expansion do not include the NXT records to prove the nonexistence of a non-wildcard match or a more specific wildcard match.

- Secure resolution

  Basic support for validation of DNSSEC signatures in responses has been implemented but should be considered experimental.

  When acting as a caching name server, BIND Version 9 is capable of performing basic DNSSEC validation of positive as well as nonexistence responses. This functionality is enabled by including a `trusted-keys` clause containing the top-level zone key of the DNSSEC tree in the configuration file.

  Validation of wildcard responses is not currently supported. In particular, a "`name does not exist`" response will validate successfully even if the server does not contain the NXT records to prove the nonexistence of a matching wildcard.

  Proof of insecure status for insecure zones delegated from secure zones works when the zones are completely insecure. Privately secured zones delegated from secure zones will not work in all cases, such as when the privately secured zone is served by the same server as an ancestor (but not parent) zone.

  Handling of the CD bit in queries is now fully implemented. Validation is not attempted for recursive queries if CD is set.

- Secure dynamic update

  Dynamic updating of secure zones has been partially implemented. Affected NXT and SIG records are updated by the server when an update occurs. Use the `update-policy` statement in the zone definition for advanced access control.

- Secure zone transfers

BIND Version 9 does not implement the zone transfer security mechanisms of RFC 2535 because they are considered inferior to the use of TSIG or SIG(0) to ensure the integrity of zone transfers.

3.4 tcpdump Restrictions

In many ways, tcpdump works the same way on OpenVMS as it does on UNIX systems, with the following restrictions:

- On UNIX systems, tcpdump sets the NIC into promiscuous mode and everything in the transmission is sent to tcpdump.

  On OpenVMS systems, tcpdump only sees the packets destined for and sent from the local host. Therefore, tcpdump works in copy-all mode. Because it only sees a copy of the the packets that are processed by the TCP/IP kernel, tcpdump can only trace natively IP, IPv6, and ARP protocols on Ethernet.

  tcpdump can format or filter packets that have been traced from another platform running tcpdump in promiscuous mode. In this case it will process other protocols, like DECnet.

- Ethernet is the only supported type of NIC. Other types of NICS (such as ATM, FDDI, Token Ring, SLIP, and PPP) are not supported.

- The -i option is not supported. On UNIX systems, this option specifies the interface that tcpdump is attached to.

  On OpenVMS systems, tcpdump obtains packets from the TCP/IP kernel.

- The -p option is not supported.

  On UNIX systems, this option specifies that tcpdump stops working in promiscuous mode.

  On OpenVMS, tcpdump does not work in promiscuous mode. Therefore, this option is set by default.

- If you are using the Ethereal software to dump IPv6 network traffic, use the following command format to write the data in the correct format:

  ```
  $ tcpdump -w filename
  ```

- Only one process at a time can issue traces. This is a common restriction for both TCPTRACE and tcpdump.

3.5 SSH Restrictions

This section contains the following information:

- General SSH restrictions (Section 3.5.1)
- File transfer restrictions (Section 3.5.2)
- Restrictions in the use of the SSH_ADD utlity (Section 3.5.3)

3.5.1 General SSH Restrictions

This section describes restrictions not specific to a particular SSH application.

- If hostbased authentication does not work, the SSH server may have failed to match the host name sent by the client with the one it finds in DNS. You can check whether this problem exists by comparing the output of the following commands (ignoring differences in case of the output text):
  - On the server host:

    ```
    $ TCPIP
    TCPIP> SHOW HOST client-ip-address
    ```

  - On the client host:

    ```
    $ write sys$output -
    $_ "''f$trnlnm("TCPIP$INET_HOST")'.''f$trnlnm("TCPIP$INET_DOMAIN")'"
    ```

    If the two strings do not match, you should check the host name and domain configuration on the client host. It may be necessary to reconfigure and restart TCP/IP Services on the client host.

- In this release, an SSH client user can copy its own version of the public key from an SSH server not previously contacted. To force users to use only the systemwide version of the server public key, you can perform the following steps.

  Note

  Steps 2 and 3 involve modification of system files. Therefore, it may be necessary to repeat them after a future update of TCP/IP Services.

  1. Edit TCPIP$SSH_DEVICE:[TCPIP$SSH]SSH2_CONFIG. to include the following line:

     ```
     StrictHostKeyChecking  yes
     ```

  2. Restrict user access to TCPIP$SSH_DEVICE:[TCPIP$SSH]SSH2_ CONFIG. For example:

```
$ SET SECURITY/PROTECTION=(G,W) TCPIP$SSH_DEVICE:[TCPIP$SSH.SSH2]SSH2_CONFIG.;
```

  3. Edit the SYS$STARTUP:TCPIP$SSH_CLIENT_STARTUP.COM command procedure to install the SSH server image with the READALL privilege on startup. In the following example, change the existing line to the replacement line, as indicated:

     ```
     . . .
     $     image = f$edit("sys$system:tcpip$ssh_ssh2.exe","upcase")
     $!    call install_image 'image' ""          <== existing line
     $     call install_image 'image' "readall"   <== replacement
     . . .
     ```

  4. Enable the SSH client, as described in the *HP TCP/IP Services for OpenVMS Guide to SSH*.

- When you execute remote commands on the OpenVMS SSH server, the log file TCPIP$SSH_RCMD.LOG is created in the directory defined by the logical name SYS$LOGIN for your user account. This log file must be purged manually.

- When you execute remote commands on an OpenVMS SSH client connected to a non-OpenVMS SSH server:
  - Output may not display correctly. For example, sequential lines might be offset as if missing a linefeed, as in the following example:

```
$ ssh user@unixhost ls -a
  user's password:
  Authentication successful.
  .
   ..
     .TTauthority
                 .Xauthority
                            .cshrc
                                  .dt
                                     .dtprofile
```

    To get the output to display correctly, use the following format:

    $ ssh -t [*options*] user@unixhost [*command*]

  - Commands that automatically refresh the display, such as the MONITOR utility, may not display correctly.
- The server configuration parameter PermitRootLogin is not supported.
- The client configuration parameter EnforceSecureRutils is not supported.
- There is no automatic mapping from the UNIX ROOT account to the OpenVMS SYSTEM account.
- The SSH1 protocol suite is not supported for terminal sessions, remote command execution, and file transfer operations. Parameters related to SSH1 in the server and client configuration files are ignored.
- Starting SSH sessions recursively (for example, starting one SSH session from within an existing SSH session) creates a layer of sessions. Logging out of the innermost session may return to a layer other than the one from which the session was started.
- Some SSH informational, warning, and error message codes are truncated in the display. For example:

```
%TCPIP-E-SSH_FC_ERR_NO_S, file doesn't exist
```

- Cutting and pasting from SSH terminal sessions on an OpenVMS server can cause data truncation. When this happens, the following error message is displayed:

```
-SYSTEM-W-DATAOVERUN, data overrun
```

- Some SSH log and trace output messages, and informational, warning, and error messages display file specifications as UNIX path names.
- From a UNIX client, if you use OpenVMS syntax for names (such as device names), enclose the names in single quotation marks to prevent UNIX-style interpretation of certain characters.

  For example, in the following command, UNIX interprets the dollar sign ($) in the device name SYS$SYSDEVICE:[*user*] as SYS:[*user*].

  # ssh *user@vmssystem directory* SYS$SYSDEVICE:[*user*]

To avoid this problem, enter the command using the following format: formats:

```
# ssh user@vmssystem directory 'SYS$SYSDEVICE:[user]'
```

- The translation of the system logical name SYS$ANNOUNCE is displayed after authentication is complete. In this version of SSH, no automated mechanism exists for displaying this text as a prelogin banner.

  To provide a prelogin banner from a text file, create the file SSH_BANNER_MESSAGE. containing the text to be displayed before login.

  To enter multiple lines in the banner text, make sure each line ends with an explicit carriage-return character except the last line.

  Save the banner message file in the TCPIP$SSH_DEVICE:[TCPIP$SSH.SSH2] directory, with privileges that allow it to be read by the user account [TCPIP$SSH].

  If you do not use the default file name and location for the message banner file, define them using the BannerMessageFile option in the TCPIP$SSH_DEVICE:[TCPIP$SSH.SSH2]SSHD2_CONFIG. file. Specify the location and file name of your banner message file as the argument to the option using one of the following formats:

  ```
  BannerMessageFile   TCPIP$SSH_DEVICE:[TCPIP$SSH]BANNER1.TXT
  BannerMessageFile   /TCPIP$SSH_DEVICE/TCPIP$SSH/BANNER2.TXT
  BannerMessageFile   /etc/banner3.txt
  ```

  Note that the argument may be in either OpenVMS or UNIX format and is not case sensitive. (If multiple definitions for the same option are included in the configuration file, the last one listed will take effect.)

  The UNIX path /etc is interpreted by the OpenVMS SSH server as TCPIP$SSH_DEVICE:[TCPIP$SSH].

- After you execute an SSH remote command, you might need to press the Return key to get back to the DCL prompt.

- When you log out, the message "Connection to *hostname* closed." may overwrite the last line of the logout message, as in the following example from an SSH session established with host tst1:

  ```
  $ LOGOUT
  Connection to tst1 closed.at  7-AUG-2003 14:37:15.01
  ```

- You cannot shut down an OpenVMS system from an SSH session, such as by executing the command:

  ```
  $ @SYS$SYSTEM:SHUTDOWN.COM
  ```

  In this version of SSH, the phase of shutdown that stops user processes disconnects the SSH session.

- SSH access from a non-OpenVMS client to a user with an expired password on an OpenVMS server is controlled by the value of the AllowNonvmsLoginWithExpiredPw option in the SSHD2_CONFIG file. For more information about this option, refer to the *HP TCP/IP Services for OpenVMS Guide to SSH*.

- SSH escape sequences are not fully supported. For example, you may have to enter the Escape . exit sequence twice for it to take effect. On exit, the terminal is left in NOECHO and PASTHRU mode.

- Any OpenVMS command that refreshes the display can have unexpected results when executed as a remote SSH command. For example, the following command exhibits this behavior:

  ```
  $ MONITOR PROCESS/TOPCPU
  ```

  Executed locally, this command displays a bar chart that is continuously updated. When executed as a remote command, it displays each update sequentially. In addition, you cannot terminate the command using Ctrl/C.

3.5.2 SSH File Copy Restrictions

- On OpenVMS, setting the `ForcePTTYAllocation` keyword to YES in the SSH2_CONFIG. file can result in failures when performing file copy operations. (In other implementations of SSH, setting the keyword `ForcePTTYAllocation` to `YES` in the SSH2_CONFIG. file has the same effect as using the `-t` option to the SSH command.)
- Using the `scp` and `sftp` commands from an OpenVMS SSH client to a UNIX server running OpenSSH is not fully supported because certain operations cause the OpenVMS client to hang. The hang cannot be terminated by entering Ctrl/C and Ctrl/Y.
- File transfer is limited to OpenVMS files with the following record formats (as displayed by the DIRECTORY/FULL command):
  - STREAM_LF
  - Fixed-length 512-byte records
- Not all variants of UNIX path names are supported when referring to files on OpenVMS clients and servers.
- Using the SCP and SFTP commands from a non-OpenVMS client may have unpredictable results, depending on how the client formats the target file name and whether the client is SSH2 compatible.

3.5.3 SSH_ADD Utility Restrictions

If you do not specify the key file in the SSH_ADD command, and SSH_ADD finds no INDENTIFICATION. file, it adds only the first private key it finds in the [*username*.SSH2] directory.

3.6 LPD Restrictions

The LPD$SPOOL logical name has been removed from the software.

3.7 IMAP Dependencies

The IMAP server is limited in the number of connections an IMAP server process can handle before it forces the kernel to create a new IMAP server process. This value is set in the TCPIP$IMAP.CONF file to 25. For example:

```
Max-Connections:25
```

3.8 NSLOOKUP Over a TELNET Connection Fails Under OpenVMS V7.3-1

If you use TELNET to connect to a system where the subsystem attribute `maxbuf` is set to greater than 32767 and execute a C program that uses a C runtime call (such as `getc` or `gets`) to read data from the terminal, the C program may return a generic user IO error message rather than the specific errors returned by RMS.

To solve this problem:

- Set the subsystem attribute `maxbuf` to 32767. This is a dynamic parameter, so no reboot is required.
- Install the OpenVMS patch VMS731_RMS-V0100.
- Reset the `maxbuf` attribute to the desired value.

3.9 FTP Restrictions

The FTP server does not allow you to specify an IP address other than that of the connected client, or the specification of a privileged port, in the PORT, LPRT, or EPRT commands. Any such commands are rejected with the following error:

```
500 Illegal {PORT|LPRT|EPRT} command.
```

The FTP server and client prevent data connection "theft" by a third party. For the FTP server, this applies to passive-mode connections from an IP address other than the client's, or from a privileged port. For the FTP client, this applies to active-mode connections from an IP address other than the server's, or from a port other than port 20.

You can restore the original behavior by defining the following logical names:

Server	Client
TCPIP$FTPD_ALLOW_ADDR_REDIRECT	TCPIP$FTP_ALLOW_ADDR_REDIRECT
TCPIP$FTPD_ALLOW_PORT_REDIRECT	TCPIP$FTP_ALLOW_PORT_REDIRECT

These logical names allow you to relax the IP address and port checks independently in the FTP server and the FTP client.

3.10 Determining the TCP/IP Device Name from a Channel Assignment

OpenVMS provides several ways to determine the name of a device on a channel assignment. Using the SYS$GETDVI/SYS$GETDVIW system services, the DVI$_DEVNAM, DVI$_FULLDEVNAM, and DVI$_UNIT items all return information about the device. While the first two items provide the full device name, the DVI$_UNIT item returns only the unit number of the device. To form the complete device name, a program must prefix the unit number (as a string) with the device name and controller information. In the case of the TCP/IP device name, the programmer could add the string `BG` or `BGA`. For example, `BG + 1234` would produce the device name `BG1234:`.

The TCP/IP device name may be altered in a future release. It is good programming practice to use the DVI$_DEVNAM or DVI$_FULLDEVNAM items to obtain the full device-name string. Such programs are not based on the

assumption that the TCP/IP device name is BG*nnnn* or BGA*nnnn*, and would not be affected by any change in the TCP/IP device name strategy.

3.11 RCP Full Transparent Copy Operations

The following sections describe limitations of RCP on OpenVMS.

3.11.1 Using RCP to Transfer STREAM_LF Files

RCP on OpenVMS is best used for transferring text files. Under previous versions of TCP/IP Services, RCP converts any type of OpenVMS file that is not STREAM_LF to STREAM_LF format using the standard OpenVMS $CONVERT utility by specifying the files in the following way:

```
FILE;ORGA SEQU;RECO;CARR CARR;FORM STREAM_LF;SIZE 0;BLOCK YES
```

RCP sends the converted file using block-mode RMS file I/O (SYS$READ()) and writes the data using block-mode (SYS$WRITE()).

This behavior has been changed so that RCP does not convert FIXED or UNDEFINED format files (in addition to STREAM_LF files). You can restore the old behavior using the following logical name:

```
TCPIP$RCP_SEND_FIX_FORMAT_AS_ASCII
```

If this logical name is set, the original behavior of converting FIXED and UNDEFINED files is restored. If this logical name is set to a number other than 1, the default behavior is enabled. Files with a fixed-length record size that exactly matches the value of the logical name are not converted.

For example, if you set this logical name to 512, all FIXED and UNDEFINED files are converted except for files with a fixed-length record size of 512 (such as OpenVMS executable image files).

The receiving peer, if OpenVMS, always creates a file of type STREAM_LF. The RCP protocol provides no method of transferring file type information between sender and receiver. Therefore, the receiving peer has no way of knowing anything about file structure.

In an OpenVMS-to-OpenVMS transfer, if the original file was FIXED or UNDEFINED and was not converted, use the DCL command SET FILE/ATTRIBUTES to change the attributes on the resulting STREAM_LF file to correspond to the format of the original file.

For example, after transferring an OpenVMS executable image file (FIXED format with a record-length of 512 bytes), enter the following command to make it an executable image again:

```
$ SET FILE/ATTR=(RFM:FIX,LRL:512) RCP-COPIED-FILE.EXE
```

3.11.2 RCP File Size Limitations

The RCP protocol requires that the length of the file be sent as part of the protocol. The length is interpreted as a signed 32-bit integer. On OpenVMS, the file's length is determined using an RTL call to `fstat()`. Therefore, files transferred using RCP must be less than 2 GB minus 1 byte (2147483647 bytes).

In comparison, FTP does not have any of these limitations. However, FTP uses a different security model.

3.12 NFS Problems and Restrictions

The following sections describe problems and restrictions with NFS.

3.12.1 NFS Server Problems and Restrictions

- Using the `ls` command from a Solaris Version 9 client may hang the OpenVMS server with no error message on either client or server. To avoid this problem, set the nfs subsystem attribute `ovms_xqp_plus_enabled` to 7. Refer to the *HP TCP/IP Services for OpenVMS Management* guide for more information about this attribute.
- Directories in a container file system cannot be deleted, either by the TCP/IP management command REMOVE DIRECTORY or by clients. The following error message is displayed:

  ```
  no such file
  ```

- Under TCP/IP Services Version 5.3, the NFS client command "mkdir dirname.dir" used on an ODS-5 volume with the TYPELESS_DIRECTORIES export option produces a directory with the OpenVMS name "dirname.DIR;1", which is displayed back to the NFS client as simply "dirname."

  This problem has been fixed in TCP/IP Services Version 5.4. The directory is now created with the OpenVMS file specification "dirname.dir.DIR;1", which is displayed back to the client as "dirname.dir," as expected.

  Therefore, non-OpenVMS clients using an ODS-5 volume should always refer to directories according to whether or not the TYPELESS_DIRECTORIES option is in use.

  - With the TYPELESS_DIRECTORIES option, the file "dirname.DIR;1" must be referred to as "dirname".
  - Without the TYPELESS_DIRECTORIES option, the file "dirname.DIR;1" must be referred to as "dirname.dir".

  Note that you may need to change some export records, either to include the ".dir" at each directory level, or to add the TYPELESS_DIRECTORIES option.

  Client MOUNT commands must also conform to this convention.

- When performing a mount operation or starting the NFS server with OPCOM enabled, the TCP/IP Services MOUNT server can erroneously display the following message:

  ```
  %TCPIP-E-NFS_BFSCAL, operation MOUNT_POINT failed on file /dev/dir
  ```

  This message appears even when the MOUNT or NFS startup has successfully completed. In the case of a mount operation, if it has actually succeeded, the following message will also be displayed:

  ```
  %TCPIP-S-NFS_MNTSUC, mounted file system /dev/dir
  ```

- If the NFS server and the NFS client are in different domains and unqualified host names are used in requests, the lock server (LOCKD) fails to honor the request and leaves the file unlocked.

  When the server attempts to look up a host using its unqualified host name (for example, `johnws`) instead of the fully qualified host name (for example, `johnws.abc com`), and the host is not in the same domain as the server, the request fails.

To solve this type of problem, you can do one of the following:

- When you configure the NFS client, specify the fully qualified host name, including the domain name. This ensures that translation will succeed.
- Add an entry to the NFS server's hosts database for the client's unqualified host name. Only that NFS server will be able to translate this host name. This solution will not work if the client obtains its address dynamically from DHCP.

3.12.2 NFS Client Problems and Restrictions

- To get proper timestamps, when the system time is changed for daylight savings time (DST), dismount all DNFS devices. (The TCP/IP management command SHOW MOUNT should show zero mounted devices.) Then remount the devices.
- The NFS client should properly handle file names with the semicolon character on ODS-5 disk volumes. (For example, `a^;b.dat;5` is a valid file name.)

  The current version does not handle these types of file names properly; they are truncated at the semicolon.
- The NFS client included with TCP/IP Services uses the NFS Version 2 protocol only.
- With the NFS Version 2 protocol, the value of the file size is limited to 32 bits.
- The ISO Latin-1 character set is supported. The UCS-2 characters are not supported.
- File names, including file extensions, can be no more than 236 characters long.
- Files containing characters not accepted by ODS-5 on the active OpenVMS version or whose name and extension exceeds 236 characters are truncated to zero length. This makes them invisible to OpenVMS and is consistent with prior OpenVMS NFS client behavior.

3.13 IPv6 Restrictions

The following sections describe restrictions in the use of IPv6.

3.13.1 Mobile IPv6 Restrictions

The implementation of mobile IPv6 in this version of TCP/IP Services does not support binding update authentication as specified in `draft-ietf-mobileip-ipv6-15.TXT`, Section 4.4, including the authentication data sub-option defined in Section 5.6. You should limit the use of this version to testing environments that are not subject to attack, because system integrity can be compromised by accepting unauthenticated bindings.

3.13.2 6to4 Configuration is Not Supported

TCP/IP Services contains the TCPIP$IP6_SETUP.COM command procedure for configuring IPv6 on a node. The use of this procedure to configure the 6to4 tunnel mechanism is not supported in this release. Attempts to configure 6to4 with the procedure will not succeed.

3.13.3 IPv6 Requires the BIND Resolver

If you are using IPv6, you must enable the BIND resolver. To enable the BIND resolver, use the TCPIP$CONFIG.COM command procedure. From the Core menu, select BIND Resolver.

You must specify the BIND server to enable the BIND resolver. If you do not have access to a BIND server, specify the node address 127.0.0.0 as your BIND server.

3.14 TCP/IP Management Command Restrictions

The following restrictions apply to the TCP/IP management commands:

- TCP/IP Services version 5.4 introduces failSAFE IP, which obsoletes the IP cluster alias address. Consequently, the following TCP/IP management commands are no longer supported:
  - TCPIP SET INTERFACE /NOCLUSTER
  - TCPIP SHOW INTERFACE /CLUSTER

  To show interface addresses, including IP cluster alias addresses, you must use the following sequence of DCL commands:

  ```
  $ @SYS$MANAGER:TCPIP$DEFINE_COMMANDS.COM
  $ ifconfig -a
  ```

  To delete a cluster alias address from the active system, use a DCL command similar to the following:

  ```
  $ ifconfig ie0 -alias 10.10.10.1
  ```

  For backward compatibility, the following TCP/IP management commands continue to be supported:
  - SET CONFIGURATION INTERFACE /CLUSTER
  - SET CONFIGURATION INTERFACE /NOCLUSTER
  - SHOW CONFIGURATION INTERFACE /CLUSTER
- SET NAME_SERVICE /PATH

  This command requires the SYSNAM privilege. If you enter the command without the appropriate privilege at the process level, the command does not work and you are not notified. If you enter the command at the SYSTEM level, the command does not work and receive an error message.
- SET SERVICE command

  When you modify parameters to a service, disable and reenable the service for the modifications to take effect.

3.15 NTP Problems and Restrictions

- NTP uses a slew mechanism to synchronize the system clock. The method that NTP uses to obtain a maximum slew value (the maximum amount that NTP will adjust the clock in one attempt) changes when you upgrade from NTP Version 3 to NTP Version 4. As a result of this change, it may take longer for clocks to come into synchronization under NTPv4 than it did under NTPv3.

- The NTP server has a stratum limit of 15. The server does not synchronize to any time server that reports a stratum of 15 or greater. This may cause problems if you try to synchronize to a server running the UCX NTP server, if that server has been designated as "free running" (with the `local-master` command). For proper operation, the `local-master` designation must be specified with a stratum no greater than 14.
- Whenn running on certain high-performance Alpha systems, NTP may be unable to adjust the system clock; therefore, NTP will not be able to provide accurate timekeeping. When this happens, the following error message appears in the NTP log file:

```
%SYSTEM-F-BADLOGIC, internal logic error detected
VMS timekeeping is not working as expected - can't proceed
```

3.16 SNMP Problems

This section describes restrictions to the SNMP component for this release. For more information about using SNMP, refer to the *Compaq TCP/IP Services for OpenVMS SNMP Programming and Reference* manual.

3.16.1 Incomplete Restart

When the SNMP master agent and subagents fail or are stopped, TCP/IP Services is often able to restart all processes automatically. However, under certain conditions, subagent processes may not restart. When this happens, the display from the DCL command SHOW SYSTEM does not include TCPIP$OS_MIBS and TCPIP$HR_MIB. If this situation occurs, restart SNMP by entering the following commands:

```
$ @SYS$STARTUP:TCPIP$SNMP_SHUTDOWN.COM
$ @SYS$STARTUP:TCPIP$SNMP_STARTUP.COM
```

3.16.2 SNMP IVP Error

On slow systems, the SNMP Installation Verification Procedure can fail because a subagent does not respond to the test query. The error messages look like this:

```
   .
   .
   .
Shutting down the SNMP service... done.

Creating temporary read/write community SNMPIVP_153.
Enabling SET operations.
Starting the SNMP service... done.
SNMPIVP: unexpected text in response to SNMP request:
"- no such name - returned for variable 1"
See file SYS$SYSDEVICE:[TCPIP$SNMP]TCPIP$SNMP_REQUEST.DAT for more
details.
sysContact could not be retrieved.  Status = 0
The SNMP IVP has NOT completed successfully.
SNMP IVP request completed.
Press Return to continue ...
```

You can ignore these types of messages in the IVP.

3.16.3 Using Existing MIB Subagent Modules

If an existing subagent does not execute properly, you may need to relink it against the current version of TCP/IP Services to produce a working image. Some subagents (such as those for OpenVMS support of Compaq Insight Manager) also require a minimum version of OpenVMS and a minimum version of TCP/IP Services.

The following restrictions apply:

- In general, only executable images linked against the following versions of the eSNMP shareable image are upward compatible with the current version of TCP/IP Services:
  - UCX$ESNMP_SHR.EXE from TCP/IP Services Version 4.2 ECO 4
  - TCPIP$ESNMP_SHR.EXE from TCP/IP Services Version 5.0A ECO 1

  Images built under versions other than these can be relinked with one of the shareable images, or with TCPIP$ESNMP_SHR.EXE in the current version of TCP/IP Services.
- The underlying eSNMP API changed from DPI in Version 5.0 to AgentX in the current version of TCP/IP Services. Therefore, executable images linked against older object library versions of the API (*$ESNMP.OLB) must be relinked against either the new object library or the new shareable image. Linking against the shareable image ensures future upward compatibility and results in smaller image sizes.

  Note

  Although images may run without being relinked, backward compatibility is not guaranteed. These images can result in inaccurate data or run-time problems.

- This version of TCP/IP Services provides an updated version of the UCX$ESNMP_SHR.EXE shareable image to provide compatibility with subagents linked under TCP/IP Services Version 4.2 ECO 4. Do not delete this file.
- The SNMP server responds correctly to SNMP requests directed to a cluster alias. Note, however, that an unexpected host may be reached when querying from a TCP/IP Services Version 4.*x* system that is a member of a cluster group but is not the current impersonator.
- The SNMP master agent and subagents do not start if the value of logical name TCPIP$INET_HOST does not yield the IP address of a functional interface on the host when used in a DNS query. This problem does not occur if the server host is configured correctly with a permanent network connection (for example, Ethernet or FDDI). The problem can occur when a host is connected through PPP and the IP address used for the PPP connection does not match the IP address of the TCPIP$INET_HOST logical name.
- Under certain conditions observed primarily on OpenVMS VAX systems, the master agent or subagent exits with an error from an internal `select()` socket call. In most circumstances, looping does not occur. You can control the number of iterations if looping occurs by defining the TCPIP$SNMP_SELECT_ERROR_LIMIT logical name.

- The MIB browser provided with TCP/IP Services (TCPIP$SNMP_REQUEST.EXE) supports getnext processing of OIDs that include the 32-bit OpenVMS process ID as a component. However, other MIB browsers may not provide this support.

  For example, the following OIDs and values are supported on OpenVMS:

  ```
  1.3.6.1.2.1.25.4.2.1.1.1321206828 = 1321206828
  1.3.6.1.2.1.25.4.2.1.1.1321206829 = 1321206829
  1.3.6.1.2.1.25.4.2.1.1.1321206830 = 1321206830
  ```

  These examples are from hrSWRunTable; the hrSWRunPerfTable may be affected as well.

- You can ignore the following warning that appears in the log file if a null OID value (0.0) is retrieved in response to a Get, GetNext, or GetBulk request:

  ```
  o_oid; Null oid or oid->elements, or oid->nelem == 0
  ```

3.16.4 Upgrading SNMP

After upgrading to the current version of TCP/IP Services, you must disable and then enable SNMP using the TCPIP$CONFIG configuration command procedure. When prompted for "this node" or "all nodes," select the option that reflects the previous configuration.

3.16.5 Communication Controller Data Not Fully Updated

When you upgrade TCP/IP Services and then modify an existing communication controller, programs that use the communication controller might not have access to the updated information.

To ensure that programs like the MIB browser (SNMP_REQUEST) have access to the new data about the communication controller, do the following:

1. Delete the communication controller using the TCP/IP management command DELETE COMMUNICATION_CONTROLLER.
2. Reset the communication controller by running the TCPIP$CONFIG.COM command procedure and exiting.
3. Restart the program (such as SNMP) by entering the following commands:

   ```
   $ @SYS$STARTUP:SNMP_SHUTDOWN.COM
   $ @SYS$STARTUP:SNMP_STARTUP.COM
   ```

4. Use the TCP/IP management command LIST COMMUNICATION_CONTROLLER to display the information.

3.16.6 SNMP MIB Browser Usage

If you use either the -l (loop mode) or -t (tree mode) flag, you cannot also specify the -m (maximum repetitions) flag or the -n (nonrepeaters) flag. The latter flags are incompatible with loop mode and tree mode.

Incorrect use of the -n and -m flags results in the following messages:

```
$ snmp_request mynode.co.com public getbulk -v2c -n 20 -m 10 -t 1.3.6.1.2.1
Warning: -n reset to 0 since -l or -t flag is specified.
Warning: -m reset to 1 since -l or -t flag is specified.
1.3.6.1.2.1.1.1.0 = mynode.company.com
```

3.16.7 Duplicate Subagent Identifiers

With this version of TCP/IP Services, two subagents can have the same identifier parameter. Be aware, however, that having two subagents with the same name makes it difficult to determine the cause of problems reported in the log file.

3.16.8 eSNMP Programming and Subagent Development

The following notes pertain to eSNMP programming and subagent development.

- In the documentation, the terms **extension subagent**, **custom subagent**, and **user-written subagent** refer to any subagent other than the standard subagents for MIB-II and the Host Resources MIB, which are provided as part of the TCP/IP Services product.
- In the [.SNMP] subdirectory of TCPIP$EXAMPLES, files with the .C, .H, .COM, .MY, and .AWK extensions contain additional comments and documentation.
- The TCPIP$SNMP_REQUEST.EXE, TCPIP$SNMP_TRAPSND.EXE, and TCPIP$SNMP_TRAPSND.EXE programs are useful for testing during extension subagent development.
- For information about prototypes and definitions for the routines in the eSNMP API, see the TCPIP$SNMP:ESNMP.H file.

4
Corrections

This chapter describes some of the user-visible problems corrected in this version of TCP/IP Services.

4.1 Management Command Interface Problems Fixed in This Release

The following TCP/IP Services TCP/IP management command problems are fixed in this release:

- **Problems:**
  - The SET CONFIGURATION ENABLE SERVICE command fails when processing node-specific or cluster-wide configuration records containing large numbers of service entries.
  - The SET CONFIGURATION ENABLE SERVICE command fails to output any error message when trying to add a service to a configuration record that already contains the maximum number of service entries.
  - The TCPIP$CONFIG.COM configuration procedure generates errors processing service lists that exceed the 1024-byte limit of DCL symbols.
  - The number (63) of service entries that can be stored in node-specific or cluster-wide configuration records is too low.

  Solutions:
  - In TCPIP$CONFIG.COM, routines correctly handle long enable service lists that exceed the 1024-byte limit of DCL symbols.
  - In TCPIP$UCX.EXE, the routine that signals "TOOMANYSERV" errors has been corrected.

    The maximum number of service entries has been changed from 64 to 128 when updating a configuration record that specifies a limit that is less than the current maximum.
  - In TCPIP$ACCESS_SHR.EXE, raised the maximum number of service entries supported in configuration records from 64 to 128.
  - In TCPIP$ACCESS_SHR.EXE, the largest record field in the record descriptor table uses the largest record size in the INET facility.

    This change corrects the system failure experienced when creating large service lists.
  - In TCPIP$MESSAGE.MSG, the TOOMANYSERV message has been added.
- **Problem:** The TCP/IP management command MOUNT generates an access violation when trying to perform a wildcarded mount operation.

Solution: MOUNT command handling and processing has been corrected.

4.2 BIND Problems Fixed in This Release

The following BIND/DNS problems are fixed in this release:

- **Problem:** A user has no way to manually flush dynamic updates with BIND Version 9.

  Solution: The `rndc flush-updates` command has been added to trigger the same behavior that the `rndc stop` command did, without actually stopping or shutting down the server.

4.3 FTP Problems Fixed in This Release

The following FTP problems are fixed in this release:

- **Problem:** Seven FTP client/server problems.

  Solution: If the device for a user in the UAF is a rooted logical, that logical must be assigned systemwide with the translation attribute at least concealed, or else the `cd` command will fail. For example:

  – moxie$root is assigned /SYSTEM only:

  ```
  FTP> cd ~moxie
  550-Failed to set default directory to
  MOXIE$ROOT:[user].
  550 error in directory name
  ```

  – moxie$root is assigned /SYSTEM/TRANSLATION=CONCEALED:

  ```
  FTP> cd ~moxie
  250-CWD command successful.
  250 New default directory is MOXIE$ROOT:[user]
  ```

  For systems with a version of DECC$SHR.EXE at or later than V7.2, assigning the following logical name enables recursive directory listings for the `ls` and `dir` commands:

  ```
  $ ASSIGN/SYSTEM 1 TCPIP$FTPD_DIR_RECURSIVE
  ```

  Turning on this flag results in the following UNIX-like behavior. Here the default directory is DEV1$:[TOPDIR] and it contains a subdirectory SUB1.DIR which contains three files:

  ```
  FTP> ls sub1
  200 PORT command successful.
  150 Opening data connection for sub1 (16.20.208.97,52062)

  DEV1$:[TOPDIR.SUB1]a.txt;1
  DEV1$:[TOPDIR.SUB1]b.txt;1
  DEV1$:[TOPDIR.SUB1]c.txt;1
  ```

  To get to the login directory of a user using *~username* format, you need system privileges if *username* is other than that of the current user.

- **Problem:** There is no way to suppress the file size in the 150 opening data connection message. The new behavior affects file transfers using an older version of SmartTerm.

  Solution: A new logical, TCPIP$FTPD_NO_FILESIZE_HINT, allows users to suppress the file-size hint added to the "150 Opening data connection..." message.

- **Problem:** The FTP client starts up in Extended parse mode. The SHOW PROCESS/PARSE command shows that the parse style is set to Extended.

  Solution: This behavior has been correct so that traditional parsing is used by default. To change the parsing style, enter the SET PROCESS/PARSE command.

4.4 NFS Problems Fixed in This Release

The following NFS server problems were fixed in this release:

- **Problems:**
  - When file names of the form *string.string.nnn* are created on an ODS5 volume, *nnn* is treated as a file version number. Viewed locally, the file appears as xxx.yyy;123 instead xxx.yyy.123;1. If the numeric part is greater than 32767, the file creation failed.
  - When creating a directory name of the form *string*.dir on an ODS5 volume with the `typeless_directories` option, the server absorbs the ".dir" part of the name. Viewed locally, the directory appears as "dirname.DIR;1" instead of "dirname.dir.DIR;1," and is displayed back to the client as "dirname" instead of "dirname.dir".
- **Problem:** The NFS client recieves errors -RMS-F-CRMP and -SYSTEM-F-SHMNOTCNCT after doing a SET FILE /STATISTICS command followed by an attempt to open the file using the COPY or TYPE command.
- If a UNIX client accesses a non-STREAM_LF file that was created by an OpenVMS client within the inactivity timer limit, the server does not do data conversion.

4.5 TELNET Problems Fixed in This Release

- **Problem:** The TELNET symbiont puts log files into SYS$SPECIFIC:[SYSEXE] even when the TCPIP$LPD_ROOT logical name is defined.

  Solution: The TCPIP$LPD_SPOOL logical name has been replaced by the TCPIP$LPD_ROOT logical name.
- **Problem:** Starting with TCP/IP Services V5.1, local echoing no longer occurs when you use TELNET to connect to a non-TELNET service (such as SMTP).

  Solution: The behavior used in earlier versions of TCP/IP Services has been restored.

4.6 SMTP Problems Fixed in This Release

The following SMTP problems are fixed in this release:

- **Problem:** The SMTP EXPN and VRFY commands are considered a security hole by many customers.

  Solution: Four new SMTP.CONFIG Allow-* options govern whether the commands are accepted or not. The *-Text options are the optional user-defined text strings to send to the client when the command is rejected. The new configuration options are:
  - Allow-EXPN

  - Allow-VRFY
  - EXPN-Used-Text
  - VRFY-Used-Text

  For more information see the *HP TCP/IP Services for OpenVMS Management* guide.

- **Problem:** Mail messages with lines beginning with a period (.) are delivered with an extra dot included.

  Solution: The period-removal code is restored. It applies only to mail message data received using the RFC 821 protocol over the wire and not from SFF (send-from-file).

4.7 SNMP Problems Fixed in This Release

The following SNMP problems are fixed in this release:

- **Problems:**
  - An attempt to send an SNMPv2 trap through TCPIP$SNMP_TRAPSND is either ignored or causes the system to fail.
  - SNMP_REQUEST `-i`, `-r`, and `s` options are ignored.

5
Documentation Update

This chapter describes updates to the information in the TCP/IP Services for OpenVMS product documentation.

5.1 Updated Documentation

The following manuals have been updated for this version of TCP/IP Services:

- HP TCP/IP Services for OpenVMS Installation and Configuration (AA-LU49O-TE)
- HP TCP/IP Services for OpenVMS Management (AA-LU50N-TE)
- HP TCP/IP Services for OpenVMS Guide to SSH (AA-RVBUA-TE)
- HP TCP/IP Services for OpenVMS User's Guide (AA-PC27L-TE)
- HP TCP/IP Services for OpenVMS Tuning and Troubleshooting (AA-RN1VB-TE)
- HP TCP/IP Services for OpenVMS Management Command Quick Reference Card (AV-RN1WB-TE)
- HP TCP/IP Services for OpenVMS Management Command Reference (AA-PQQGI-TE)
- HP TCP/IP Services for OpenVMS UNIX Command Equivalents Reference Card (AV-RNJ4B-TE)
- HP TCP/IP Services for OpenVMS Guide to IPv6 (AV-RNJ3B-TE)

In addition, this version of TCP/IP Services includes new version of the Help files:

- HELP TCPIP_SERVICES
- TCPIP HELP
- HELP FTP
- HELP TELNET
- HELP NSLOOKUP
- HELP/MESSAGES

The following manuals are not updated for TCP/IP Services V5.4:

- Compaq TCP/IP Services for OpenVMS Sockets API and System Services Programming
- Compaq TCP/IP Services for OpenVMS SNMP Programming and Reference
- Compaq TCP/IP Services for OpenVMS ONC RPC Programming and Reference
- Compaq TCP/IP Services for OpenVMS Concepts and Planning

These manuals will be updated in a future release of TCP/IP Services. For this release, use the existing manual with the changes described in the following sections.

5.1.1 SNMP Programming and Reference Update

The following information will be added to the *Compaq TCP/IP Services for OpenVMS SNMP Programming and Reference* manual:

- The trap communities configured for regular SNMP through the TCPIP$CONFIG.COM command procedure, the TCP/IP management command SET CONFIG SNMP, or in the SYS$SYSDEVICE:[TCPIP$SNMP]TCPIP$VMS_SNMP_CONF.DAT file are not used to determine the trap receiver host or community name.

  The values of the `-c` and `-h` flags to the SNMP_TRAPSND utility are handled as follows:

  - If no `-c` (community) flag is used, the default name "public" is used in the trap.
  - If no `-h` (host) flag is used, the trap is sent to LOCALHOST.

- The value for the "agent address" field in the SNMPv1 trap PDU is that of the primary interface for the host on which the master agent (TCPIP$ESNMP_SERVER) is running. The value of this address can be verified as follows:

  1. Translate logical name TCPIP$INET_HOSTADDR
  2. Obtain the value of LOCALHOST using the following TCP/IP management command:

     ```
     $ TCPIP SHOW CONFIGURATION COMMUNICATION
     ```

     If this value is not in IP address format, determine the IP address using the following command:

     ```
     $ TCPIP SHOW HOST/LOCAL local-host-name
     ```

5.1.2 Sockets API and System Services Programming Update

The information in the *Compaq TCP/IP Services for OpenVMS Sockets API and System Services Programming* manual will be updated as follows:

- Table 2-2 describes the default setting for the TCPIP_KEEPIDLE option incorrectly. The default setting for this option is 7200 seconds (14400 half seconds). In addition, the manual fails to mention that, in order to use the options in Table 2-2, your program must use the TCP.H file.

5.2 Help Files Update

The HELP CC Socket_Routines information has been removed. Instead, the information about socket programming is provided when you enter the following command:

```
$ HELP TCPIP_SERVICES Programming_Interfaces Sockets_API
```

The Sockets_API HELP file has been enhanced with IPv6 information.